



UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/780,997	02/09/2001	Ken Kutaragi	SCEI 18.303	5883

26304 7590 04/19/2007
KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER

PATEL, NIRAV B

ART UNIT	PAPER NUMBER
----------	--------------

2135

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 09/780,997	Applicant(s) KUTARAGI ET AL.	
	Examiner Nirav Patel	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 January 2007 (Amendment).
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7,9-12 and 14-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7,9-12 and 14-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's amendment filed on January 30, 2007 has been entered. Claims 9 and 10 are amended by the applicant. Claims 1-7, 9-12 and 14-22 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-7, 9-12, 14-17, and 19-20 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatesan et al, US Patent No. 6898706B1, herein after "Venkatesan", in view of Matsumoto et al, US Patent No. 6286008, hereinafter "Matsumoto".

As per Claim 1:

Venkatesan discloses "A method of providing a content, characterized in that:

when a content is transmitted to a user, an electronic watermark for preventing execution of said content is embedded in said content and at least information associated with the user, to whom said content is to be transmitted, is added to said content; and

when said content is executed, said information associated with the user who has received said content is checked at a transmitting end

Art Unit: 2135

when said content is executed, said information associated with the user is checked at a receiving ends; and

the execution of said content is allowed by removal of said electronic watermark if and only if the result of the checking indicates that said content is an authorized content” in (Col 22 lines 36-54);

(59) Subsequently, when the user stationed at the client PC attempts to access any watermarked object, the client PC, as indicated in block 590, will access the encrypted object, C.sub.i, from encrypted store 580 (or, if the object does not then reside in store 580, will prompt the user to either download that object from the publisher's web site or insert a diskette containing that object into the client PC for subsequent access). Assuming the encrypted object then resides within store 580, that object will be accessed as symbolized by line 587. In addition, the client PC, through execution of block 590, will determine whether a license (L.sub.i) then exists in license database 570 for this object. If such a license is found, the license is accessed as symbolized by line 577. Thereafter, block 590 will verify the license and, if the license is valid, decrypt the object, appearing on line 587, and instruct the O/S in client PC.sub.j to utilize the resulting decrypted fingerprinted, watermarked object in accordance with the rights specified in the license.

However, Venkatesan does not teach of “when said content is executed, said information associated with the user is checked at a receiving ends;”

Nevertheless, Matsumoto discloses a method of deciphering content if the client *apparatus is authenticated with server* and receiving user information from the server to authenticate at the client” in (Col 11 line 60 to Col 12 line 30).

(12) In the server side apparatus 2, when the user ID UID and data C(R1, Su) are received from the user side apparatus 1 through the communication line 3 (Step S21), the execution program EP2 causes a common secret information search unit 41 to search the user ID UID of plural users registered and stored in a data base 42 to have it take out the corresponding registered common secret information Ss from the registered common secret information (Step S22). And, the execution program EP2 causes a data inverse conversion unit 43 to convert inversely the received data C(R1, Su) with the registered common secret information Ss taken out from the data base 42 to obtain a random number R1 (Step S23).

(13) Next, in the server side apparatus 2, the execution program EP2 newly causes to generate the random information (random number) R2 (Step S24), and the random number R1 obtained by the data inverse conversion unit 43 and the

Art Unit: 2135

random number R2 are concatenated, the resulting data is read out from the data base 42, and using the registered common secret information Ss read out from the data base 42, the concatenated data is converted by a data conversion unit 44 to generate a data C(R2//R1, Ss) (Step S25), which is caused to transmit to the user side apparatus 1 through the communication line 3 (Step S26).

(14) At the time when the data C(R2//R1, Ss) is generated in the data conversion unit 44, if money charging processing is necessary, such processing is executed.

(15) When this data C(R2//R1, Ss) is received (Step S15), in the user side apparatus 1, the execution program EP1 causes a data inverse conversion unit 32 to make inverse conversion with the common secret information Su inputted previously by the user himself to obtain a random number R1 (Step S16). The execution program EP1 compares the random number R1 obtained in the data inverse conversion unit 32 with the random number R1 generated previously by its own at the comparing unit 33 (Step S17), and if they show coincidence, then the program starts the self-uncompression program UP to have the compressed contents CC start to be uncompressed (Step S18).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Venkatesan's invention to incorporate Matsumoto's teaching of authenticate request to the server and also authenticate again at the local host prior decrypting the watermarked content. The Matsumoto's teaching adds additional security layer for accessing the content and also preventing the pirate copy of the watermarked content being executed without any knowledge of the provider.

As per Claims 7 and 12:

Venkatesan discloses "A content providing system according to one of Claims 4 and 5, wherein: when the information associated with a user received from a user terminal is registered, in advance, in the user database of said content provider, said content provider transmits to said user a card on which a card ID is stored" in (Col 15 lines 5-18, Media card and Card ID is the watermark key); and Matsumoto discloses "said

Art Unit: 2135

information associated with the user includes at least a user name, a password, a device ID uniquely assigned to a device of said user, and said card ID" in (Col 11 lines 60-67).

As per Claims 1-5, 9-10, 14-15 and 22:

Venkatesan discloses "A content provider connected to at least one user terminal via a network, said content provider comprising:

a content server which stores plural kinds of digital contents" in (Col 11 lines 1-10); and

"a user database for registering, in advance, information associated with a user received from said at least one user terminal" in (Col 16 lines 60-67), wherein:

when said content provider receives from a user terminal a request for providing a particular content, said content provider requests said user terminal to resend the information associated with said user and transmits the requested content:" in (Col 22 lines 5-35); and

(57) Subsequently, the user, through client PC.sub.j, establishes an Internet session with the publisher's web server and as, indicated by block 540, electronically transacts with that server to obtain a license to use the previously downloaded object. In that regard, the user is presented through a web page generated by the publisher's web server with a menu, list or other graphical selection mechanism through which (s)he can select an extent to which (s)he wants to access and use that object, i.e., to obtain so-called "rights". Once the user makes the selection and authorizes electronic payment for the desired rights, the browser, based on embedded code in the web page, transmits, to the publisher's web server, the rights selection, payment authorization and a computer identification (CID) associated with client PC.sub.j. Each client PC has a unique CID. The CID can be formed, in whole or in part, by illustratively a processor serial number (PSN) that has been embedded into the processor itself, e.g., processor 420 of client PC 400 shown in FIG. 4, during its manufacture.

Art Unit: 2135

when the content transmitted from said content provider is executed, checking is performed as to whether the information associated with said user included in said content is consistent with the information stored in the user terminal, and said content provider determines, in accordance with the result of the checking, whether to transmit a content execution permission command to said user terminal" in (Col 22 lines 35-54);

(59) Subsequently, when the user stationed at the client PC attempts to access any watermarked object, the client PC, as indicated in block 590, will access the encrypted object, C.sub.i, from encrypted store 580 (or, if the object does not then reside in store 580, will prompt the user to either download that object from the publisher's web site or insert a diskette containing that object into the client PC for subsequent access). Assuming the encrypted object then resides within store 580, that object will be accessed as symbolized by line 587. In addition, the client PC, through execution of block 590, will determine whether a license (L.sub.i) then exists in license database 570 for this object. If such a license is found, the license is accessed as symbolized by line 577. Thereafter, block 590 will verify the license and, if the license is valid, decrypt the object, appearing on line 587, and instruct the O/S in client PC.sub.j to utilize the resulting decrypted fingerprinted, watermarked object in accordance with the rights specified in the license.

wherein: said content provider further includes encryption means for encrypting the information associated with a user and embedding an electronic watermark in said content for preventing execution of said content, and, when said content provider receives from a user terminal a request for providing a particular content, said content provider transmits the requested content after combining the requested content with the information associated with said user and with the electronic watermark" in (Col 22 lines 17-35); and

(58) Once this information is transmitted to the publisher's web server, that server issues, as indicated by block 550 shown in FIG. 5, an electronic license (L.sub.i) and transmits, as symbolized by line 555, that license to the client PC. This license, which is signed by the publisher, specifies, among other parameters--which have been alluded to above and will be discussed in detail below, the specific rights of access and use that have been accorded to client PC.sub.j for the downloaded object along with a secret key to decrypt this object. This key, as previously noted, is a symmetric encryption key, i.e.,

Art Unit: 2135

the same key previously used by the publisher to encrypt the object. Upon receipt of this license, the browser routes this license, as symbolized by line 565, to encrypted store 610 and specifically stores this license, within license database 570, for subsequent access. Store 570 contains a repository of licenses for each watermarked encrypted object which the user has downloaded to client PC.sub.i or otherwise has in his possession and desires to access through this PC.

Venkatesan discloses a capability of checking the which user associates to which client pc through the use of PCID in the user database in (Col 16 lines 55-67)

However, Venkatesan does not discloses "wherein said content execution permission command transmitted from said content provider serves to remove said electronic watermark for allowing execution of said content.

said information associated with said user after checking that said information associated with said user is consistent with the information registered in said user database"

Nevertheless, Matsumoto discloses a method of authenticating to the server from a client apparatus, wherein user information is transmitted to the server for authentication. Once the authentication at the server is successful, the server transmitting back an authorization to authenticate at the client apparatus before allowing the deciphering of the watermarked or encrypted content for execution" in (Col 11 line 60 to Col 12 line 30).

(12) In the server side apparatus 2, when the user ID UID and data C(R1, Su) are received from the user side apparatus 1 through the communication line 3 (Step S21), the execution program EP2 causes a common secret information search unit 41 to search the user ID UID of plural users registered and stored in a data base 42 to have it take out the corresponding registered common secret information Ss from the registered common secret information (Step S22). And, the execution program EP2 causes a data inverse conversion unit 43 to convert inversely the received data C(R1, Su) with the registered common secret information Ss taken out from the data base 42 to obtain a random number R1 (Step S23).

Art Unit: 2135

(13) Next, in the server side apparatus 2, the execution program EP2 newly causes to generate the random information (random number) R2 (Step S24), and the random number R1 obtained by the data inverse conversion unit 43 and the random number R2 are concatenated, the resulting data is read out from the data base 42, and using the registered common secret information Ss read out from the data base 42, the concatenated data is converted by a data conversion unit 44 to generate a data C(R2//R1, Ss) (Step S25), which is caused to transmit to the user side apparatus 1 through the communication line 3 (Step S26).

(14) At the time when the data C(R2//R1, Ss) is generated in the data conversion unit 44, if money charging processing is necessary, such processing is executed.

(15) When this data C(R2//R1, Ss) is received (Step S15), in the user side apparatus 1, the execution program EP1 causes a data inverse conversion unit 32 to make inverse conversion with the common secret information Su inputted previously by the user himself to obtain a random number R1 (Step S16). The execution program EP1 compares the random number R1 obtained in the data inverse conversion unit 32 with the random number R1 generated previously by its own at the comparing unit 33 (Step S17), and if they show coincidence, then the program starts the self-uncompression program UP to have the compressed contents CC start to be uncompressed (Step S18).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Venkatesan's invention to incorporate Matsumoto's teaching of authenticate request to the server and also authenticate again at the local host prior decrypting the watermarked content. The Matsumoto's teaching adds additional security layer for accessing the content and also preventing the pirate copy of the watermarked content being executed without any knowledge of the provider.

As per Claim 11:

Matsumoto discloses "A content providing system according to one of Claims 9 and 10, wherein said information associated with the user includes at least a user name, a password, and a device ID uniquely assigned to a device of said user" in (Col 11 lines 60-67).

Art Unit: 2135

As per Claims 16 and 19:

Venkatesan discloses "The method of claim 1, wherein when the result of the checking indicates that said content is an authorized content, key information for removal of said electronic watermark is transmitted to the user" in (Col 15 lines 5-20).

As per Claims 17 and 20:

Venkatesan discloses "The method of claim 16, wherein the key information represents a data location of said content at which the electronic watermark is embedded" in (Abstract).

3. Claims 18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatesan et al, US Patent No. 6898706B1, herein after "Venkatesan", in view of Matsumoto et al, US Patent No. 6286008, hereinafter "Matsumoto", and further in view of Ishii, US Patent No. 5768389.

As per Claims 18 and 21:

Venkatesan does not disclose "The method of claim 16, further comprising the step of deleting the key information by the user after removal of the electronic watermark. However, Ishii discloses a method of deleting key after decrypting the data in (Col 22 lines 55-62)

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate Ishii's teaching of key deletion for safe guarding the decryption key from apprehension.

Response to Arguments

4. Applicant's arguments filed January 30, 2007 have been fully considered but they are not persuasive.

Applicant argues that:

Neither Venkatesan nor Matsumoto discloses *checking information at a transmitting end*. Therefore, neither Venkatesan nor Matsumoto teach the execution of contents that is allowed by removal of an electronic watermark *if the result of both checking step at transmitting and receiving ends* indicates that the contents are authorized content.

Examiner maintains that:

Venkatesan discloses a BORE resistant object (content) is created by embedding a relatively large number of identical watermarks throughout a single software object, through use of different secret watermark key. Whenever the client compute attempts to access a file containing a protected object, the enforcer examines the object using its secret watermark key. Further, the client operating system accesses a license database to determine whether a signed license made to the enforcer and linked, via the publisher's cryptographic signature, to this protected object resides in that database [Fig. 5]. Therefore, Venkatesan teaches checking/verifying the access rights (or license

Art Unit: 2135

information) at the client computer at the time of execution. In addition, Venkatesan teaches the authorization process at the server side before issuing the license to the client computer **[Fig. 11]**. Matsumoto's invention relates to a method of distributing content (software) after certain processing (e.g. compression, enciphering, etc.). Fig. 7-9 and Fig. 10-12 are illustrating the processing procedures of the user side apparatus 1 and the processing procedures of the server side apparatus 2. When the data $C(R2//R1, Su)$ presented by the execution program, the execution program EP1 causes it to transmit to the server side apparatus 2 through the communication line (Step S36). When the server side apparatus receives the data $C(R2//R1, Su)$ from the user side apparatus, the secret information search unit search the user ID (UID) of plural users stored by registration in advance in the database 42 according to the user ID previously received **[col. 12 lines 61-67, col. 13 lines 1-11]**. Further, *in the server side apparatus, the execution program EP2 causes a comparing unit to compare the random number R1 taken out by the data inverse conversion unit 43 with the random number R1 previously transmitted to the user side apparatus (Step S47) and if they show coincidence (i.e. checking/verifying the information at the server/transmitted end)*, then the new generated random number transmitted to the user side apparatus **[col. 13 lines 13-26]**. When the data is received, **in user side apparatus, the comparing unit compares the random number obtained in the data inverse conversion unit with the random number previously generated and if they show coincide (i.e. checking/verifying the information at the user/receiving end)**, then it starts the self-uncompression program and have the uncompression of the

Art Unit: 2135

compressed contents started [col. 13 lines 30-40]. Therefore, Matsumoto teaches a *dual checking system (i.e. checking at the transmitted end and checking at the receiving end) when the content is executed at the user/receiving end*. In this case, the combination of Venkatesan and Matsumoto teaches the claimed subject matter and the combination is sufficient.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

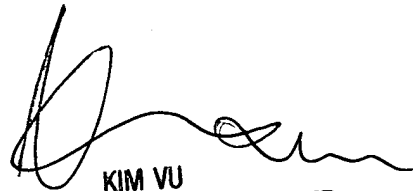
5. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP

4/4/07


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100